


A Generic Construction of Tightly Secure Password-based Authenticated Key Exchange*

Jiaxin Pan 

Runzhi Zeng 

September 7, 2023

Department of Mathematical Sciences,
NTNU Norwegian University of Science and Technology, Trondheim, Norway
jiaxin.pan@ntnu.no, runzhi.zeng@ntnu.no

Abstract

We propose a generic construction of password-based authenticated key exchange (PAKE) from key encapsulation mechanisms (KEM). Assuming that the KEM is *oneway secure against plaintext-checkable attacks (OW-PCA)*, we prove that our PAKE protocol is *tightly secure* in the Bellare-Pointcheval-Rogaway model (EUROCRYPT 2000). Our tight security proofs require ideal ciphers and random oracles. The OW-PCA security is relatively weak and can be implemented tightly with the Diffie-Hellman assumption, which generalizes the work of Liu et al. (PKC 2023), and “almost” tightly with lattice-based assumptions, which tightens the security loss of the work of Beguinet et al. (ACNS 2023) and allows more efficient practical implementation with Kyber. Beyond these, it opens an opportunity of constructing tight PAKE based on various assumptions.

Keywords: Password-based authenticated key exchange, generic constructions, tight security, lattices

Breaking down the concept that a KEM is One-Way Secure against PCA (OW-PCA):

1) One Way Security: This basically means that it should be computationally infeasible for an adversary to reverse an encapsulation operation. In case of KEMs, when a KEM ciphertext is generated by encapsulating a secret value, an adversary must not be able to retrieve the (encapsulated) secret value only from the KEM ciphertext or any data related to the KEM ciphertext.

2) The concept of Plaintext Checkable Attacks (PCA) simply refers to a scenario where, an adversary is able to query a decryption oracle to verify whether a guessed plaintext is the correct one, i.e., does this guessed plaintext match the secret value which was encapsulated using the KEM.

3) Security against OW-PCA means that, even if an adversary has access to a decryption oracle against which he can verify guesses of different plaintext, he should still not be able to efficiently reverse the KEM encapsulation process and find the plaintext which matches the secret value.

In simpler terms, it should be infeasible for an adversary to derive the secret value without the respective private key, even with the availability of the ciphertext or any data related to the ciphertext.

*Supported by the Research Council of Norway under Project No. 324235.